MobileIron Core Delegated Administration Guide 10.8.0.0

August 31, 2020

Contents

New Features and Enhancements

This guide documents the following new features and enhancements:

- **Filter users by LDAP OU in device registration, Spaces, and Labels**: You can now include Lightweight Directory Access Protocol (LDAP) Organizational Units (OU) within Space and Label criteria, restricting the results to the users in that OU. This feature set includes the following updates:
  - **LDAP OUs in space and label criteria**: You can now create device spaces and labels based on LDAP OUs. There is a new attribute in the **Admin > Device Spaces > New Admin Space >** "Field" menu: **Organizational Units > LDAP Organizational Unit Distinguished Name** (OUDN). If you select this option, a list of LDAP Organizational Units populates the right-hand drop-down menu, from which you can configure your criteria. See Filtering users by OUs and groups.

Overview

About delegated administration

Delegated administration enables IT administrators to decentralize the management of MobileIron Core devices. Dividing a MobileIron Core system into several areas of influence enables primary Core administrators to maintain control over all critical areas of system management and also give limited control of specific areas of the system to other administrators. This feature is MobileIron's solution to segmented administrative challenges, allowing administrators to create flexible, dynamic rules and administrative capabilities for a defined subset of users.

Device Spaces

Using delegated administration with MobileIron Core, administrators are assigned areas of influence called device spaces. Device spaces can represent departments or offices locations other than the main office, or other selected groups of the company. To delegate administration tasks, administrators are assigned roles that define what administrative tasks they can perform, and which devices, labels, policies, apps and configurations they can manage.

Device spaces allows IT administrators to partition groups of devices and/or users for separate management based on specific criteria such as device characteristics or LDAP Group.

Delegated Administration and Role-Based Access:

- Enables organizations to efficiently support distributed locations, user groups, and devices.
- Enables organizations to create of different “spaces” to help partition groups of devices and/or users, and to assign administrators the permission to view or manage spaces.

The original device space in MobileIron Core is called the global space. If you do not use delegated administration, this is the only device space in your Core system. Administrators assigned to the global space can be assigned any roles. Administrators assigned to other device spaces are assigned fewer roles.

Designing MobileIron Core to use delegated administration

If you have a reason to assign different policies, labels, configurations, or apps to a group such as help desk workers or executive staff, then you have a reason to create a device space for that group and assign an administrator or group of administrators to manage the devices and users in that device space.

When you design a MobileIron Core system that uses delegated administration, there are questions you need to answer about your Core system. The first task is to decide how you want to divide your system into device spaces. For example, you could create a device space for:

- Help desk groups in your company (Help Desk France, Help Desk Germany)
- Business units (West Coast Sales, HQ Finance)
- Countries where your company has offices (England Office, Holland Office)

Your Core system can support any combination of these device space types and more.

After you decide what device spaces to create, plan what tasks the administrators assigned to each device space will perform. For example:

- Do you want to give administrators in the Toronto office the ability to view the devices and users assigned to that office, or should they be able to perform additional tasks, such as wiping all corporate apps from the devices they manage?
- Do you want to give your front-line help desk workers in Texas the ability to view application details for their callers' devices?
- Should administrators in the Sydney office be able to assign labels and policies to the devices they manage?
- Should administrators in the Sydney office be able to add a set of their Apps and Configurations, and distribute it to the devices they manage?

Once you answer these and other questions about your MobileIron Core system, study the available roles and permissions presented in “Administrator roles” in the *Getting Started with MobileIron Guide* to determine which roles to assign each group of administrators in each device space.

Using roles, you can create administrative tiers within a device space. Suppose you set up device spaces for different countries (for example, the United States, Germany and France). You could then create two help desk administrator groups for each device space, one for front-line workers, who have minimal permissions and one for back-line workers, who have additional permissions. To this scenario, you could also add the ability for a local administrator to assign policies and configurations. You can also assign the distribute apps role to the space administrators.

You need to think about the reasons why you would segment your user population. These needs will guide how you set up your device spaces.

Delegated administration setup prerequisites

Before setting up delegated administration in your MobileIron Core system, assess your needs for labels. This is true if you are setting up a new installation or if you are adapting an existing installation. See *Label & Device Spaces Best Practices*: https://community.mobileiron.com/docs/DOC-4903

Creating Administrator roles

Administrator types

For delegated administration, MobileIron Core is managed by two types of administrators.

- **Global Administrators**, who also manage devices throughout your MobileIron Core system. These administrators are assigned to the global space and can be assigned any roles.
- **Device Space Administrators**, who manage only the devices and users assigned to the device spaces to which they are assigned. For example, an administrator assigned to the Dallas Help Desk device space can only manage devices assigned to that device space. The roles that can be assigned to Device Space Administrators are limited. For example, Device Space Administrators, if assigned the correct role, can view configurations or apply and remove configurations from a label. Device Space Administrators, can create and edit configurations and apps. Device Space Administrators can only add, search, or view users and devices that belong in their own space. They can also send messages to devices and apps within their own space.

For complete information about roles and actions available to each type of administrator, see “Administrator roles” in the *Getting Started with MobileIron Guide*.

Creating device spaces and assigning administrators

Global Administrators are the only administrators that can create, edit and delete device spaces, assign and remove administrators, and assign roles and permissions to and remove them from administrators.

Assigning an administrator to a device space enables that administrator to manage devices assigned to that device space. The administrative tasks that the administrator can perform depend on the roles assigned to that administrator. Administrators can be assigned to more than one device space and can have different roles and permissions in each assigned device space.

NOTE: Although Global Administrators have roles that enable them to perform specific tasks, they can perform these tasks only in device spaces to which they are assigned. By default, these administrator types are assigned to the global space, but not to individual device spaces.

Creating device spaces is a two-step process.

First, you name the device space (for example, France Android) and define criteria that determine which devices belong to the device space (for example, all Android devices used in the France help desk group).

Second, you select the administrators for the device space and assign them the roles they need to perform the management actions you have chosen for administrators in this device space.

When creating device spaces:

- MobileIron recommends that you assign administrators to the new device space and assign them the roles necessary for their planned management tasks before closing the dialog. Assigning administrators and roles later limits you to adding administrators and roles one at a time rather than as a group.
- Using the New Admin Space dialog, you can only select one set of users and assign them one set of roles.
- For devices assigned to device spaces, an administrator assigned the necessary roles can view the name of the device space to which the device is assigned in the Devices page.

After deciding how to use delegated administration in your MobileIron Core system, create the device spaces, assign administrators to the device spaces, and then assign roles to the administrators using the following procedure:

1. In Admin Portal, go to **Admin > Device Spaces**.
2. Click **Add+** to add a device space.
3. Enter the name for the device space in **Space Name**.
4. To specify which devices are assigned to the device space, create a query using the **All** and **Any** buttons and the Fields, Operators and Values fields displayed (see Specifying devices for device spaces on page 6 for details).
5. Click **Save** to create the device space and move to assigning administrators to the device space.
6. To assign administrators to the device space, complete one of the following actions:

- Click **LDAP Entities**, select LDAP OU, LDAP Groups, or LDAP Users, and then enter one or more characters in the search box below LDAP Entities to display a list of LDAP users that meet the search criteria (see Filtering users by OUs and groups for details).
- Click **Individual Admins**, and then enter one or more characters in the search box next to **Individual Admins** to display a list of local users that meet the search criteria.

7. Select the device space administrators from the list.
8. Select roles for the device space administrators from the lists of roles in the dialog (see "Editing administrator roles" in the *Getting Started with MobileIron Guide* for information about the available roles and permissions). When you select a role from one of the categories, Device Management for example, the permissions for the selected role move from the Available Permissions column to the Selected Permissions column. If the permissions associated with a role are included in a previously selected role, no permissions are added to the Selected Permissions column.

NOTE: The new device space status is Pending after you click Save. Until the status of all device spaces is Active rather than Pending, the device counts for the device spaces are not reliable and devices may not be listed in the correct device space.

Updating device spaces

Updating device spaces involves several MobileIron Core actions:

- Update device space
- Device space evaluation
- LDAP synchronization

You update device spaces after creating spaces or changing device space priority. MobileIron recommends that you wait until you finish creating all your device spaces, including assigning administrators and roles, or complete changing device space priority before you update device spaces. This saves system resources.

To update device spaces:

1. Finish creating your device spaces or complete changing device space priorities.
2. Click **Update Spaces Now**.
   MobileIron Core displays a message that it might take several hours to update Core with the new device space. The actual time it will take to update Core with the new device space depends on the number of devices assigned to the device space, the priority of the new device space and how it affects the priorities of the other device spaces in Core.

Specifying devices for device spaces

This section explains how to use the query tool available in the New Admin Space dialog to select devices for device spaces. When specifying the criteria for selecting devices for a device space, follow these instructions to use the search tool provided in the New Admin Space dialog:

NOTE: This procedure assumes that you are already defining a device space using the New Admin Space dialog.

1. Click **Any** or **All** to specify whether the search result includes devices that meet one or more of the conditions (Any), or must meet all the specified conditions (All).
2. Click the **Field** drop-down menu, navigate to the search field and select it (see Switching device spaces on page 9 for the list of available fields).

   NOTE: Type a few letters of the field name to display a list of matching fields, or press the Expand All button within the field list to display all possible fields.
3. In **Operator**, select one of the possible operators for the selected field.
4. In **Value**, select or enter the value for the selected search field.

   NOTE: A green icon indicates that the query syntax is correct; a red icon indicates that the syntax is incomplete or incorrect.
5. (Optional) Click the plus sign to the right of the query condition you just created to add another condition.
6. (Optional) Repeat Step 2 through Step 5 for each additional query.
7. (Optional) To remove a condition from the search criteria, click the minus sign to the right of that condition.
8. A sample listing of the devices that meet the query criteria is displayed below the query as you complete each condition.
9. Check the sample device list to ensure that the query results are returning the types of devices you intended. The sample list contains up to twenty devices. To test that the search criteria returns all the devices to be included, run the same query using MobileIron Core advanced search in the **Devices** tab.

Filtering users by OUs and groups

Expect the following behaviors and limitations when filtering users with these combinations of Organizational Units (OUs) and groups:

TABLE 1. BEHAVIORS AND LIMITATIONS

User filtering criteria one	Operation	User filtering criteria two	Behaviors and Limitations
OU or group	AND	OU or group	User filtering based on OU criteria is not applied. All (name-matching) users are listed. (Limitation)
OU or group	AND	Another user or device rule	Only the LDAP OU rule is applied. The other rule is not applied. (Limitation)
OU or group	OR	OU or group	Filtering from both criteria is applied. Users belonging to either of the search options are listed.
OU or group	OR	Another user or device rule	No user filtering is applied. All (name-matching) users are listed.

Searchable fields

The fields available as search criteria for devices assigned to a device space are divided into six categories: Android Fields, Common Fields, Custom Attributes, iOS Fields, User Fields and Windows Fields.

- User Fields specify which users are connected with the devices.
- Android Fields, Common Fields, iOS Fields, and Windows Fields are device related fields.
- Custom Attributes are for user or device related fields to associate additional properties.

For example:

To select an LDAP Field for the search item:

1. Select **User Fields** and then **LDAP**.
   The choices listed for the search field depend upon how your LDAP server is set up.
2. Select one of the following to specify the search field:
   - User Attributes, which lets you select a user attribute, such as displayName, as a search field
   - LDAP User Locale
   - Principal
   - upn
   - Groups, which lets you specify an LDAP group
   - LDAP User Distinguished Name
   - LDAP Organizational Units Distinguished Name
   - Attribute Distinguished Name

To select a Device Field for the search item:

1. Use the **Field** drop-down menu to select a device category.
   - Android Fields
   - Common Fields
   - Custom Attributes: Custom Attributes are added by going to **Settings > Custom Attributes** (in the Users & Devices section). Click **Add+** to add values for the Custom Device Attribute or the Custom User Attribute.
   - iOS Fields
   - Windows Fields
2. Click the arrow to left of the field type to specify a search parameter.
   For example select **Common Fields > Serial Number** to add "common.SerialNumber" = "" as a search parameter.

Some administrator tasks are only available to administrators assigned to the global space. Only administrators assigned to the global space who are assigned the necessary roles can:

- Create and edit device spaces
- Assign and remove administrator roles
- Assign administrators to and delete them from device spaces
- Access the V1 API
- Access the Settings and Services pages

Switching device spaces

If you use delegated administration, all administrators will see a device space list at the top right of the Admin Portal. The list contains all the device spaces assigned to that administrator. The device spaces list is shown when an administrator has permission in more than one space. Using this list, administrators can easily switch between spaces without logging out and then logging in again.

To switch device spaces:

1. Click the device space list at top right of the Admin Portal.
2. Select the device space you want to manage next.

Managing device spaces

Managing device spaces for your MobileIron Core system can include:

- Managing device space priority
- Deleting device spaces
- Editing device spaces
- Assigning and removing administrators from device spaces, including the global space
- Changing the roles assigned to device space administrators

Device space information for your MobileIron Core system is displayed when you go to **Admin > Device Spaces**. The information displayed includes:

TABLE 2. DEVICE SPACE INFORMATION

Column	Description
Space Name	Name given to device space
Criteria	Query that defines which devices are assigned to the device space
Admins	Administrators assigned to the device space
Status	Current status of the device space
Number of Devices	Number of devices currently assigned to the device space
Priority	Device space priority

Managing device space priority

Device spaces are assigned a priority when you create them. The first device space you create has the highest priority, which is Priority 1. The second device space you create has Priority 2.

Go to **Admin > Device Spaces** to view the priorities of device spaces. The priority of each device space is listed in the Priority column.

NOTE: The global space is always assigned the lowest priority among the device spaces.

You can change device space priority at any time. To change device space priority:

1. In Admin Portal, go to **Admin > Device Spaces**.
   The device spaces are listed in priority order. The device space with the highest priority is listed first.
2. Select the device space to change.
3. Drag the device space entry to the new priority position in the list. For example, to move HQ Space from the highest priority to the third-highest priority, select HQ Space from the list of device spaces and drag it to the third position in the list.
4. Click **Update Spaces Now** to complete the device space change.

NOTE: Until MobileIron Core completes the device space priority change, the number of devices in each device space is unreliable. When the status of all device spaces is Active, the update is complete and the device counts are correct for each device space.

Deleting device spaces

You can remove device spaces from MobileIron Core. When you delete device spaces from Core:

- Devices assigned to the deleted device space are assigned to a different device space. The device space each device is assigned to depends on the device criteria for the other device spaces in MobileIron Core and device space priority. For example, if DeviceA needs reassignment, Core checks whether DeviceA meets the criteria for inclusion in the highest priority device space. If DeviceA does not meet that device space's criteria, Core continues down the priority list of device spaces until it finds the highest-priority device space for which DeviceA qualifies.

NOTE: Devices that do not meet the criteria for any other device space are assigned to the global space.

- Administrators assigned to the deleted device space are not reassigned. If they are administrators in other device spaces, those assignments remain. However, if they are not assigned as administrators in other device spaces, they no longer have any administrator roles or permissions.

To delete device spaces:

1. In Admin Portal, go to **Admin > Device Spaces**.
2. Check the box next to the name of the device space to delete.
   You can select and delete one or more device spaces.
3. Click **Actions** and select **Delete Space.**
4. Click **Yes** to confirm deleting the device space.
5. Click **Update Spaces Now**.

NOTE: The status of all devices assigned to the deleted device space is Pending until MobileIron Core processes the deletion. However, devices registered with Core after you delete the device space are not assigned to the deleted device space.

While the **Delete Space** action is processed, actions such as **Force Device Check-in**, **Change Language** and **Change Ownership** cause devices assigned to the deleted device space to change device spaces immediately.

Therefore, while the status of devices assigned to the deleted device space is Pending and various device actions are occurring, device counts for all device spaces are unreliable.

Assigning administrators to spaces

MobileIron suggests that you add administrators to device spaces when you add device spaces to MobileIron Core. The New Admin Space dialog enables you to assign a group of administrators to a device space and assign them the necessary roles. Assigning administrators after a device space is added allows you to add only one administrator at a time.

To assign an administrator to a space:

1. In Admin Portal, go to **Admin > Admins**.
2. In the **To** field, select **Authorized Users** or **LDAP Entities**.
3. If you selected:
   - **LDAP Entities**, select an LDAP category (LDAP Groups, LDAP OU, LDAP Users), and then specify criteria in Search by Name for the LDAP user to assign as an administrator.
   - **Authorized Users**, enter criteria in Search by Name to find the local user to assign as an administrator.
4. Click **Enter** to run the search, and then select one local or LDAP user from the search results.
5. Go to **Actions > Assign to Space**.
6. From **Space Name,** select the device space that the selected user will manage.
7. Assign roles to the administrator for that device space (see “Editing administrator roles” in the *Getting Started with MobileIron Guide* for role and permission details).
8. Click **Save**.

NOTE: You cannot save the device space assignment until you assign the administrator at least one role.

Editing device space criteria

As an Admin you can edit device spaces to customize the criteria to your needs. You must have Admin privileges for the space you want to edit.

To edit a device space:

1. In the Admin Portal, go to **Admin > Device Spaces**.
   If you cannot access the Admin tab you cannot edit the device space.
2. Select the device space to edit.
3. Select **Edit Space** from the **Actions** drop-down menu to display the **Edit Space** page.
4. Enter the new **Name** for the space you wish to edit.
5. Use the text field in the **Criteria** section to edit the existing criteria. Click **Save**.
   The space goes into a pending state while the new criteria is being applied.

Labels and delegated administration

Delegated administration enables administrators to create labels and to assign other administrators the roles to view, apply and remove labels. This section describes label behavior in MobileIron Core systems using delegated administration.

- Within a device space, you can view both local and global labels. However, from a device space you cannot edit global labels or apply and remove them.
- The Labels page has a new column, Space, that lists the device space where the label was created (either global or a device space name).
- Label names are unique within a MobileIron Core. For example, you cannot have a label named *Android* in the global space and another label named *Android* in the device space *Boston Help Desk*.
  MobileIron Core enforces this restriction. For example, suppose an administrator creates a label for the device space *Boston Help Desk*, and gives it the name *HelpDesk*. If another administrator in a different device space attempts to create a label named *HelpDesk*, Core returns an error message to the second administrator, stating that label name is already in use in Core.
- Local labels can be deleted only from the device space in which they are defined.
- Global labels can be deleted only from the global space.You can save labels from an advanced search so they can be applied later to policies or configurations.

Managing Apps

As a Global or Space administrator you can perform the following actions in your space:

- Add Apps in your space
- Configure Apps in your space
- Delete Apps in your space
- Manage iBooks in your space

A new Space column has been added to the App Catalog page and the iBooks page to identify the spaces where the app is associated. The Space column is only shown when there is more than one space that is available. The Space column shows the spaces name where an app configuration is available.

- Only the Global Admin can manage and distribute apps utilizing Apple licenses by applying or removing a label. The Space Admin cannot use any manage Apple license functionality.
- Only the Global Admin can add or edit a Managed App configuration of an app that is included in the Global space. The Space Admin cannot modify the Managed App Configuration of an app.
- Only the Global Admin can has the ability to add or modify the Android enterprise restrictions. The Space Admin cannot modify the Android enterprise restrictions.
- Only the Global Admin can add, edit or delete a web app. The Space Admin cannot create, edit or delete new web apps, but the Space Admin can apply or remove labels for web apps.

The Global Admin can enable the Distribute app catalog role for a Space Admin. This gives the Space Admin the ability to manage apps in the app catalog within their space. They have the permission to add, edit, or delete an app. To enable the ability to manage the app catalog for the Space Admin:

1. Select a Space Admin.
2. Click **Actions > Edit Roles** to display the **Edit Roles** screen.
3. Select the **Distribute App or Import and edit app** check box in the **App Management** drop-down menu.
4. Click **Save**.

To make an app available to Android enterprise, you must have Android enterprise registered on MobileIron Core. Only the Global Admin can make an app available to Android enterprise container. The Space Admin cannot apply labels or change the priority and modify the Android enterprise restrictions.

1. Select a space using the drop-down menu on the right.
2. Go to **Apps > App Catalog**.
3. If needed, click **Add+** to display the available App Catalogs to add an app to the space.
4. Select an app catalog and use the search function to find the app.
5. Click **Continue** to display the app Preview page.
6. Optionally, use the **Category** drop-down to add a new category for the app.
7. Click **Next**.
8. Choose whether or not to display the app in the Apps@Work catalog or add the app in the featured banner. Apps@Work apps have the same functionality in the Global space or in a subspace.
9. Optionally, select to apply the Per App VPN for the Label in the Per App VPN Settings section.

Managing the App Catalog

You can define the Global Admin's or the Space Admin's permission to manage apps by checking **Manage App**, **Distribute app**, or **Import and edit app** in the **App Management** section of the **Edit Roles** page.

1. Go to **Admin > Admins** and click the check for an Admin.
2. Click **Actions > Edit Roles**.
3. Scroll down to the **App Management** section and select the permission to grant to the Admin.

Importing Apps into a Space

With the current updates, the Space admin can import an app. If an admin tries to upload an app that is already in either active or global space, an error message is displayed. If the admin uses Quick Import then the re-import option is displayed.

If the app exists in a different subspace, but not in the Global space, then the Space admin can import the app and configure it for the space.

If the app already exists in the Global Space and has a global app configuration applied, the space admin can click on the app and use the **Save As** button to add it to the subspace and configure it in the subspace.

To import an app:

1. As a Global or Space Admin, go to **Apps > App Catalog.**
2. If needed, select an admin space using the drop-down menu in the upper right corner or log into your space.
3. Click **Quick Import > (select the appropriate App store).**
4. Enter any part of an application name or bundle ID.
5. Click **Search**. Search results from the app store you selected are displayed.
6. Click **Import**, at the end of the line, to add the app to the App Catalog.
   You can also re-import the app if it already exists in another space.
7. Click **X** to close the dialog box.

Uploading a new In-house App into a Space

You can upload an in-house app that does not already exist in the Global space or in any other space. Also, if the app exists in a different subspace, but not in Global space, then the Space Admin can upload the app and configure it for the space.

The provisioning profile will be shared across spaces. If a provisioning profile is uploaded for an application by the Space Admin, the profile will be shared across all spaces thatuse that application.

APNS certificate is space-specific. For an application, every space can upload their own APNS certificate.

Use the Import procedure to import the app. To upload a new app please see, Updating Apps in a Space on page 16

Editing Apps in a Space

A Global or Space Admin can use the **Save As** button to load a copy of the current app configuration to edit and save the new configuration in their space. A Global or Space Admin can upload an in-house app into the space and edit the configuration to produce a unique app configuration for the subspace. The Space Admin will still be able to see the app configuration for the same app that exists in the Global space. If an app has a Global app configuration, a Space app configuration and a Label criteria (for example, iOS) is applied to the Global app configuration, then the devices in that subspace will receive the space app configuration even without applying the label in space.

To edit an app in a space:

1. In App Details page all the spaces where the app config is available will be listed on the left hand side.
2. Select a space name from the list on the left to display the corresponding app configuration details.
3. If the current space is same as selected space, then the user will have an option to edit the app configuration by clicking the **Edit** button.
   Administrators can only edit their own space configuration and are not allowed to edit other space configurations.
4. If the app does not have configuration in current space then Space Admin can do a Save As of any other listed space configuration. Select the app and click **Save As** to make the appropriate changes to the app configurations.

NOTE: The Space Admin cannot change the name of the app or the app description. The Space Admin cannot do a Save As from an app imported in another subspace.

Deleting Apps from a Space

A Global Admin or Space Admin can delete an app from their own space. A Space Admin can delete an app in the subspace, but the app will not be deleted from other subspaces under the control of other Space Admins. If the app also exists in the Global space with a global app config it will not be deleted from the global space. Only the Global Admin can delete a global app and the global app config. The label association of an app is removed when the parent configuration is removed.

When an app is removed from a space, the app and the app configuration specific to that space is removed immediately. The app will be removed from the catalog only when the last space configuration is removed. When the space configuration of an app is removed and the global space has a configuration for that app:

- The applied labels for that app in the space will not be removed unless there are no configurations for the app in the global space.
- The devices in that space will receive the global configuration of that app.The last configuration removed can either be the Global configuration or the Space configuration.

The user can select multiple apps to delete. The User will be allowed to delete the apps only if all the apps selected have a configuration in that space.

To delete an app from a space:

1. Select the app or apps you want to delete and click **Actions** drop-down menu.
2. Click **Delete**. A confirmation dialog is displayed.
3. Click **Yes** to delete the app you selected.

NOTE: The app will be deleted from the device. APNS certificate and the provisioning profile is deleted as well. All the different versions of the same In-House App uploaded to different spaces share the same APPCONNECTCONFIG, APPCONNECTPOLICY and PROVISIONINGPROFILE.

Managing Apps in the Android enterprise container

The Global Admin controls which apps are available in the Android enterprise container and whether or not to make an app available in another space.

- In the Android enterprise page, select the **Install this app for Android enterprise** checkbox. This selection cannot be changed by the Space Admin.
- The Space Admin cannot change any of the other configuration settings of the app in the Android enterprise container including **Auto Update this App**.
- The Space Admin can see the Android enterprise restrictions added by the Global Admin but can not edit or delete them.
- If the Space Admin distributes an app it must be as an Android enterprise app or Windows Business Store Portal (BSP) app.
- If the Global Admin deletes an app then any copies of the app must be changed so that it is no longer an Android enterprise app.

Managing Windows Business Store Portal apps in the Delegated Administration spaces

Using and managing Windows Business Store Portal (BSP) apps follow the same rules and restrictions as other apps in the Global Admin or Space Admin environment. For information on enabling and using Windows BSP apps see "*Business Store Portal*" in the *MobileIron Core 9.5.0.0 Device Management Guide for Windows Devices*.

Uploading content to iBooks iOS app

As a Global or Space admin you can upload content to an iBooks iOS app.

To upload content to iBooks:

1. Go to the Admin portal.
2. Go to **Apps > iBooks**.
3. Click **Add+** to display the Add Content page.
4. Use the radio button to select the Document Type.
5. Use the **Browse ...** button to upload the file.
6. Enter the Title and Author.
7. Use the radio buttons to select a file format.
8. Click **Save**.

Updating Apps in a Space

You can enable or disable automatic updates for an app within a space. When auto-update is enabled, the description, name and screenshots will be updated automatically.

If automatic updates are enabled in the global space, the name and description of the app will be updated in the subspaces as well, even if auto-update is disabled in the subspace by the Space Admin, as these fields are shared across all spaces.

To update apps in a space:

1. As a Global or Space Admin, go to the Admin portal. Use the drop-down menu in the upper right to select the space you administer.
2. Go to Apps and select the App.
3. Click **Edit**.
4. In the Advanced Settings section of Managed App Settings, select the **Automatically update app when a new version is available** checkbox. This is available to the Global Admin only.

NOTE: The device will be notified when an app version update is available from the spaces where this attribute is enabled.

Managing Policies

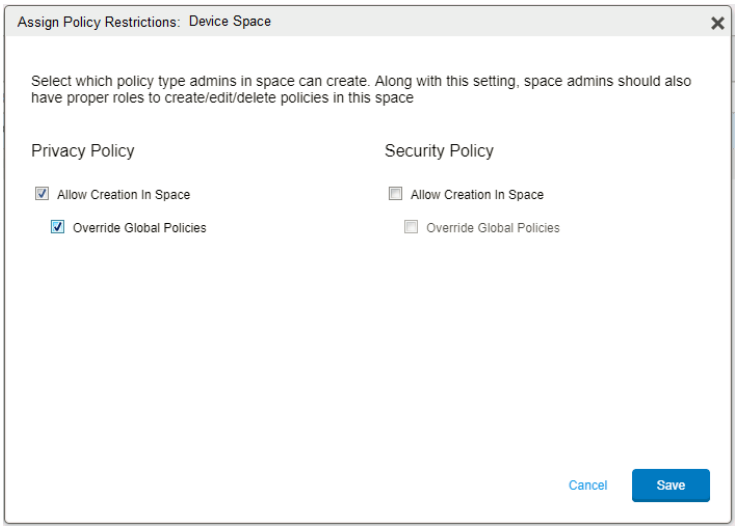
Delegated administration support is extended to manage policies in a device space. Space admin can add, edit, delete, modify policy priority, and distribute policies from their spaces.

Creating custom policies in a device space

Creating custom policies in a device space is similar to creating policies in a global space. The policies created in a device space is usable only in that space. The policies created in a subspace by the space admin cannot be used in the global space.

To manage policies in a device space, the space admin should have **Manage Policy** role and the global admin should have enabled the space admin to create a specific policy in his custom space by checking **Allow Creation in Space** for that specific policy in the **Admin > Device Space > Select the Space > Actions > Assign Policy Restriction** page. The following figure displays the Assign Policy Restriction and Override Global Policy option.

FIGURE 1. ASSIGN POLICY RESTRICTION AND OVERRIDE GLOBAL POLICY



The priorities of the newly created policies in a space is based on the Override or No Override rule. The policy override control option lets the device space admin **Override Global Policies**. The Global space admin can select any of the following override options:

- **Override Global Policies** - If global admin selects this option for a particular space and policy type, then all the space policies of that type will have higher priority than the policies of same type from global space.
- **Do Not Override Global Policies** - If global admin does not select the Override Global Policies option, then the space policies of the selected type will have lesser priority than the global policies of same type.

Policy Priorities in Device Space

In a device space, the priorities of all the space and global policies are listed. The default policy created in global space has the lowest priority in all the spaces and is disabled for changing the priority. In a global space, filtering by space shows only policies related to that space without the priority column.

Device space admin can only modify priority of the policies that are created in the device space. In Modify Policy Priorities view, space admins can view all the global policy and space policy priorities but can only modify priority of the policies that are created in their device space.

To modify policy priority:

1. Click **Policies&Configs > Policies**.
2. From the **Policy Type** drop down list, select a policy type. For example, Privacy.
3. Click on **Modify Priority** option, the **Modify Policy Priorities** window opens.
4. Drag and Drop the policy rows to change the priority.
5. Click **Save**.

Managing policies supported in Device Space

- A device space admin can view the policies in their own space and the global space. The global admin can view policies in the global space and any device space.

To filter policies by space:

a. In the Admin portal go to **Policies & Configs > Policies**
b. Click the **Filter by Space** drop-down list.
c. Select the Space to display the policies in the space.

- A new Space column has been added to the policies page to display the Device Space name associated with the selected policy. The Space column is only shown when there is a Device Space other than the Global space in the Core.
- Delegated Admin supports **Policy Management** from Device Space. The device space admin can add, update, delete, and distribute policies from his device space. Policy management from a device space works when:
  - **Manage Policy** role is enabled for their space.
  - Policy restriction for that policy type is enabled by the Global admin for device space. **Admin → Device Spaces> Actions > Assign Policy Restriction** option. Global admin enables the space admin to create a specific policy in their custom space by checking **Allow Creation in Space** for that specific policy using the **Assign Policy Restrictions** option.

NOTE: The **Assign Policy Restrictions** action appears only when there is a custom space configured in the system

- The **Add New** drop-down list **Policies & Configs> Policies**, supports the following policy types that are managed in a device space:
  - Security
  - Privacy
- Support for the following actions is available for device space admin:
  - Add
  - Edit
  - Delete

  - Apply to Label
  - Remove from Label
  - The **Save As** action is available in a subspace only when the device space admin has the **Manage Policy** role enabled and the option to create that **Policy Type** is available for that space.
  - Modify Policy Priority
- When a Global admin changes the policy restrictions of a space, the following sequence of events takes place:
  - **Disable option to create a policy type in space**: When Allow Creation in Space is disabled for a particular policy type in a space, then all policies of that type in that space will be deleted from the Core and policies would be re-evaluated and updated accordingly in the device.
  - **Change restriction from override to do not override**: If the Global admin changes the restriction from override to do not override then, the priorities of space polices will be lower than the global policies for that policy type in space, and based on the reevaluation, appropriate policy would be re-pushed to the device.
  - **Change restriction from do not override to override**: If the Global admin changes the restriction from do not override to override then, the priorities of space policies will be higher than the global policies for that policy type in space, and based on the reevaluation, appropriate policy would be re-pushed to the device.

Managing Configurations

Delegated administration support has been extended to managing configurations in a device space.

Creating a custom configuration in a device space

Creating a custom configuration in a device space is similar to creating a configuration in a global space. The configurations created in a device space is usable only in that space. The configurations created in a subspace by the space admin cannot be used in the global space.

Managing configuration supported in device space

- To manage configurations in a device space, the Manage Configuration role has been made available for a Device Space Administrator. An Administrator with this role can access the configurations tab in the Admin Portal under **Policies & Configs > Configurations**.
- A Space admin can view the configurations in their own space and the global space. The Global admin can view configurations in the global space and any device space.
  To filter configurations by space:
  a. In the Admin portal go to **Policies & Configs > Configurations**
  b. Click the **Spaces** drop-down list.
  c. Select the Space to display the configurations in the space.
- A new Space column has been added to the Configurations page to display the device space name associated with the selected Configuration. The Space column is only shown when there is any device space other than the global space in the Core.
- The **Add New** drop-down list **Policies & Configs> Configurations**, supports the following configurations that are managed in a device space:
  - Exchange: The option allows you to customize the exchange configuration for the device or global space .
  - Email: Securely synchronize data from back-end systems such as corporate email.
  - Wi-Fi: Enable or disable access to wireless LANs.
  - VPN: This option is used to secure network connection over a public network. A mobile device uses a VPN client to securely access protected corporate networks.
  - Certificates: The **Policies & configs> Configurations> Add New> Certificates** option allows you to create a new certificate in your device space. If the configuration is created in device space, then it is visible in device and global space only.
  - Certificate Enrollment: The **Policies & configs> Configurations> Add New> Certificate Enrollment** supports managing the following configurations in a device space:
    1. Entrust
    2. Local
    3. SCEP
    4. Symantec Managed PKI
    5. Symantec Web Services Managed PKI
- iOS Restrictions: The **Policies & configs> Configurations> Add New> iOS and macOS > iOS Only> Restrictions** option allows you to configure restriction on your iOS devices through the device space.
- Certificate Management: The **Logs > Certificate Management** is available for device space:

  - Device space admins can see and perform actions on certificates generated by their own certificate enrollment configuration.
  - Device space admins can see and perform actions on certificates generated by their own certificate enrollment configurations.
- The **Edit** button in the Configuration Details pane is enabled only if the selected configuration belongs to the current space.
- The **Delete** action from the Actions drop-down list is accessible only if the Delete Configuration role is assigned to the Administrator. The Delete button is enabled only if the selected configuration belongs to the current space.
- The Apply and Remove Label action is available if the admin has the Apply and Remove Label or Manage configuration roles. In a Global space, the admin cannot perform the Apply and Remove Label action on a subspace configuration. Hence, this action would be disabled when a subspace configuration is selected. In a subspace, admin can perform Apply/Remove Label action on his configuration as well as Global configuration.
- The **Save As** action is available in a subspace if the selected configuration is one of the supported configurations that are listed above and the Save as action itself is supported for that configuration.
- The **Export** and **Import** options are disabled in a subspace. A Global Administrator can export a configuration that belongs to a Global space or any subspace, however an import action will always result in the configuration being imported in the Global space.
- A configuration may depend on other configurations, Local CA, Certificate, Certificate Enrollment, Apps and so on. While creating a configuration the dependent configurations to be listed varies from case to case. But the general rule followed is that configurations from the current space and its parent space will be listed. Dependent configurations from child space cannot be used in parent space. This rule is an exclusion for Apps in Wi-Fi, Apps from a child space are also listed along with Apps from current and parent space.

  For more information about these configurations, see the *MobileIron Core 9.6.0.0 Device Management Guide.*

Managing Apple Licenses

Delegated administration support is extended to manage **Apple App Licenses** in a device space. The space administrator can create an Apple License account to purchase and distribute apps in their device space. The space administrator can also add, edit, delete Apple Licenses, change priority, update licenses and distribute Apple apps.

The global administrator can view the details of all the Apple Licenses in global and other custom spaces. But a space administrator can only view the details of the Apple Licenses available in the device space.

A new **Space** column has been added to **Apps> App Licenses**. The space column is only shown when there is more than one space that is available. The space column shows the name of the device space the Apple License belongs to. The space administrator can perform actions for the Apple Licenses in his device space.

Adding Apple Licenses in custom space

Adding Apple Licenses in a custom space is similar to adding Apple Licenses in a global space. The Apple Licenses added in a space is usable only in that space. This holds true for both global and sub spaces. The Apple Licenses added in a subspace by the space administrator cannot be used in the global space.

To manage Apple Licenses in a device space, the global administrator should enable the Manage App Licenses role for space admin. To assign app management role select **Admin > Admins> Select the name> Actions >Edit Roles** page.

NOTE: You cannot add the same Apple License to multiple spaces.

Managing the Apple License app distribution in device space

A space administrator can distribute Apple apps belonging to space Apple Licenses by selecting the **Manage Licenses** action in **Apps > App Catalog > Action** menu. For any Apple app, the column **Licenses Purchased/Used** will show the data only for the Apple Licenses that belong to the logged-in device space. For example, in global space the total number of Apple licenses purchased would be a sum of all the licenses from global Apple License accounts.

If a device that is consuming an Apple License from a space Apple License account moves to a different device space, the following would be the impact:-

NOTE: A device can move from one device space to another if the space criteria is changed or the space priority is changed or the current space is deleted.

- If the app is not present for distribution in the new space, the app is deleted and license is revoked from the device.

- If the app is distributable as a normal app (non-Apple License) in the new space, then the Apple app is not deleted but the Apple License is revoked for that app.
- If the app is distributable as a Apple License app in the new space, the Apple license would still be revoked for the app and a new license would not be assigned unless the app is re-installed.

When a device space is deleted, all the Apple Licenses created in the device space would also be deleted.

General Data Protection Regulation Compliance

In adherence to General Data Protection Regulation (GDPR) compliance following changes are made:

- New role to **View App inventory** has been introduced for Global space, to limit which app administrators can view app inventory list on employee devices.
  - In fresh Core instance, all users would NOT get this role by default, and need to explicitly enable this role to view the app inventory.
  - On upgrade, existing users with **Manage App** role will get this role automatically checked.
  - This role is only available for Global space.
- New role **View device IP and MAC address** has been introduced for Global space, to limit access to device IP and MAC address.
  - This role would be disabled by default, to enable the administrator needs to explicitly select this option to view the IP address.

Delegated administration feature support

This section addresses features supported for Core releases. For more information, see Label and Device Spaces Best Practices. A MobileIron support login is required.

- Global = Supported in the global space
- Device = Supported in the device space

Labels

Labels:

- Add
- Delete
- Save As

Support provided in release:

- 10.3.0.0 - Global, Device
- 10.4.0.0 - Global, Device
- 10.5.0.0 - Global, Device
- 10.6.0.0 - Global, Device
- 10.7.0.0 - Global, Device

Devices

Devices:

- Add single device
- Add multiple devices
- Export to CSV

Support provided in release:

- 10.3.0.0 - Global, Device
- 10.4.0.0 - Global, Device
- 10.5.0.0 - Global, Device

- 10.6.0.0 - Global, Device
- 10.7.0.0 - Global, Device

Apps

TABLE 3. APP FEATURES BY RELEASE

Feature	10.3.0.0	10.4.0.0	10.5.0.0	10.6.0.0	10.7.0.0
Import public app	Global Device	Global Device	Global Device	Global Device	Global Device
Upload in-house app	Global Device	Global Device	Global Device	Global Device	Global Device
Upload iBook	Global Device	Global Device	Global Device	Global Device	Global Device
Edit app	Global Device	Global Device	Global Device	Global Device	Global Device
Distribute app	Global Device	Global Device	Global Device	Global Device	Global Device
Distribute iBooks	Global Device	Global Device	Global Device	Global Device	Global Device
Delete app	Global Device	Global Device	Global Device	Global Device	Global Device
Add webapp	Global	Global	Global	Global	Global
Edit webapp	Global	Global	Global	Global	Global
Delete webapp	Global	Global	Global	Global	Global
Distribute webapp	Global Device	Global Device	Global Device	Global Device	Global Device
Manage Android enterprise Config	Global	Global	Global	Global	Global
Distribute Android enterprise app	Global	Global	Global	Global	Global

TABLE 3. APP FEATURES BY RELEASE (CONT.)

	Device	Device	Device	Device	Device
App auto update	Global Device	Global Device	Global Device	Global Device	Global Device
Managed App Config	Global	Global	Global	Global	Global
Distribute Managed App Config	Global Device	Global Device	Global Device	Global Device	Global Device
All other Configs Distribute	Global Device	Global Device	Global Device	Global Device	Global Device

Configurations

TABLE 4. CONFIGURATION FEATURES BY RELEASE

Feature	**10.3.0.0**	**10.4.0.0**	**10.5.0.0**	**10.6.0.0**	**10.7.0.0**
Manage VPN Config	Global Device	Global Device	Global Device	Global Device	Global Device
Manage Exchange Config	Global Device	Global Device	Global Device	Global Device	Global Device
Manage Email Config	Global Device	Global Device	Global Device	Global Device	Global Device
Manage iOS Restriction Config	Global Device	Global Device	Global Device	Global Device	Global Device
Manage Certificates Config	Global Device	Global Device	Global Device	Global Device	Global Device
Manage Wi-Fi Config	Global Device	Global Device	Global Device	Global Device	Global Device

Configurations > Certificate Enrollment

TABLE 5. CERTIFICATE ENROLLMENT FEATURES BY RELEASE

Feature	10.3.0.0	10.4.0.0	10.5.0.0	10.6.0.0	10.7.0.0
Entrust	Global Device	Global Device	Global Device	Global Device	Global Device
Local	Global Device	Global Device	Global Device	Global Device	Global Device
SCEP	Global Device	Global Device	Global Device	Global Device	Global Device
Symantec Managed PKI	Global Device	Global Device	Global Device	Global Device	Global Device
Symantec Web Services Managed PKI	Global Device	Global Device	Global Device	Global Device	Global Device

Configurations > Apple > iOS / tvOS

Configurations > Apple > iOS / tvOS >

- Restrictions

Support provided in release:

- 10.3.0.0 - Global, Device
- 10.4.0.0 - Global, Device
- 10.5.0.0 - Global, Device
- 10.6.0.0 - Global, Device
- 10.7.0.0 - Global, Device

Configurations > Apple > macOS Only

TABLE 6. MACOS ONLY CONFIGURATION FEATURES BY RELEASE

Feature	10.3.0.0	10.4.0.0	10.5.0.0	10.6.0.0	10.7.0.0
macOS Kernel Extensions	Global Device	Global Device	Global Device	Global Device	Global Device
macOS Restrictions	Global Device	Global Device	Global Device	Global Device	Global Device
macOS App Store Restrictions	Global Device	Global Device	Global Device	Global Device	Global Device
Disc	Global Device	Global Device	Global Device	Global Device	Global Device
Media Control	Global Device	Global Device	Global Device	Global Device	Global Device
Mobile@Work macOS Script	Global Device	Global Device	Global Device	Global Device	Global Device
Firewall	Global Device	Global Device	Global Device	Global Device	Global Device

Configurations > All other Configs

Configurations:

- Add single device
- Add multiple devices
- Export to CSV

Support provided in release:

- 10.3.0.0 - Global, Device
- 10.4.0.0 - Global, Device
- 10.5.0.0 - Global, Device

- 10.6.0.0 - Global, Device
- 10.7.0.0 - Global, Device

Policies > Policy Restrictions for Spaces

TABLE 7. POLICY RESTRICTIONS FOR SPACES FEATURES BY RELEASE

Feature	10.3.0.0	10.4.0.0	10.5.0.0	10.6.0.0	10.7.0.0
File Vault 2: Allow Creation; Override Global Policies	Global	Global	Global	Global	Global
File Vault 2 Redirect Recovery Key: Allow Creation; Override Global Policies	Global	Global	Global	Global	Global
iOS Software Update Policy: Allow Creation; Override Global Policies	Global	Global	Global	Global	Global
macOS Software Update Policy: Allow Creation; Override Global Policies	Global	Global	Global	Global	Global
Privacy Policy: Allow Creation; Override Global Policies	Global	Global	Global	Global	Global
Security Policy: Allow Creation; Override Global Policies	Global	Global	Global	Global	Global
System Policy Control Policy: Allow Creation; Override Global Policies	Global	Global	Global	Global	Global
System Policy Managed Policy Allow Creation; Override Global Policies	Global	Global	Global	Global	Global
System Policy Rule Policy Allow Creation; Override Global Policies	Global	Global	Global	Global	Global

Policies > iOS and macOS > iOS Only

Policies > iOS and macOS > iOS Only:

- Software Upgrade

Support provided in release:

- 10.3.0.0 - Global
- 10.4.0.0 - Global
- 10.5.0.0 - Global
- 10.6.0.0 - Global
- 10.7.0.0 - Global

Policies > iOS and macOS > macOS Only

TABLE 8. MACOS ONLY POLICIES FEATURES BY RELEASE

Feature	10.3.0.0	10.4.0.0	10.5.0.0	10.6.0.0	10.7.0.0
File Vault 2	Global	Global	Global	Global	Global
FileVault 2 Retrieve Personal Recovery Key	Global	Global	Global	field name changed to: File Vault 2 Redirect Recovery Key Global	Global
System Policy Control	Global	Global	Global	Global	Global
System Policy Managed	Global	Global	Global	Global	Global
System Policy Rule	Global	Global	Global	Global	Global
macOS Software Update	Global	Global	Global	Global	Global

Policies > Privacy Policy

Policies > Privacy Policy:

- Add
- Edit
- Delete

Support provided in release:

- 10.3.0.0 - Global, Device
- 10.4.0.0 - Global, Device
- 10.5.0.0 - Global, Device
- 10.6.0.0 - Global, Device
- 10.7.0.0 - Global, Device

Policies > macOS security

Policies > macOS security:

- Add
- Edit
- Delete

Support provided in release:

- 10.3.0.0 - N/A
- 10.4.0.0 - Global, Device
- 10.5.0.0 - Global, Device
- 10.6.0.0 - Global, Device
- 10.7.0.0 - Global, Device

Policies > All Policies

Policies > All Policies:

- Add
- Edit
- Delete
- Distribute

Support provided in release:

- 10.3.0.0 - Global, Device
- 10.4.0.0 - Global, Device
- 10.5.0.0 - Global, Device
- 10.6.0.0 - Global, Device
- 10.7.0.0 - Global, Device